CLAIMS

What is claimed is:

1. A system comprising:

a load balancer to receive requests from a client browser via a network, said requests dispatched by a Web page having a first frame and a second frame; and

a plurality of servers coupled to said load balancer to process said requests routed by said load balancer, each server executing a software code to generate a new uniform resource locator (URL) and return a redirect message with the new URL to said client browser in response to a request received from a requesting frame to load data object for a target frame, wherein when the client browser receives said redirect message with the new URL, the browser dispatches a new request using the new URL to the server specified by the new URL.

2. The system of claim 1, wherein said software code generates said new URL and returns said redirect message in the event the owner of the target frame is different from the owner providing the data object.

3. The system of claim 1, wherein said plurality of servers is used to host a Web site having a secured area and an unsecured area.

4. The system of claim 3, wherein at least one of Hypertext Markup Language (HTML) documents of said Web site contains a software code to automatically invoke Hypertext Transfer Protocol Secure (HTTPS) protocol when a client user enters said secured area from said unsecured area.

5. The system of claim 4, wherein said software code automatically invokes HTTPS protocol by building a new URL by concatenating https:// with the domain name of the Web site.

6. The system of claim 1, wherein said load balancer is capable of performing Secure Sockets Layer (SSL) encryption and decryption using hardware-based accelerator circuitry.

7. The system of claim 6, wherein communication between said load balancer and the plurality of servers is transmitted as cleartext.

8. A method comprising:

receiving requests from a client browser via a network, said requests

5   dispatched by a Web page having a first frame and a second frame;

routing said requests to one of servers in an array to process said requests; and

in the event (1) a request is received from a requesting frame to load data object for a target frame and (2) the owner of the requesting frame is

10   different from the owner providing the data object,

(i) generating a new uniform resource locator (URL), and

(ii) returning a redirect message with the new URL to said client browser.

9. The method of claim 8, further comprising:

15   receiving by the client browser said redirect message with the new URL transmitted by one of said servers; and

dispatching by the client browser a new request using the new URL to the server specified by the new URL.

10. The method of claim 8, wherein said servers are coupled to a load

20   balancer are used to host a Web site having a secured area and an unsecured area.

11. The method of claim 10, further comprising automatically invoking Hypertext Transfer Protocol Secure (HTTPS) protocol when a client user enters said secured area from said unsecured area.

25   12. The method of claim 11, wherein said automatically invoking is carried out by a software code embedded within a Hypertext Markup Language (HTML) document to build a new URL by concatenating https:// with the domain name of the Web site.

13. The method of claim 11, further comprising performing Secure

30   Sockets Layer (SSL) encryption and decryption in a load balancer coupled said servers when HTTPS protocol has been invoked.

20

14. The system of claim 8, wherein communication between a load balancer and the servers is transmitted as cleartext.

15. A machine-readable medium that provides instructions, which when executed by a processor, cause said processor to perform operations comprising:

receiving a request from a requesting frame of a client browser to load data object for a target frame; and

determining if the owner of the target frame is different from the owner providing the data object,

if so, then

generating a new uniform resource locator (URL), and

returning a redirect message with the new URL to said client browser.

16. The machine-readable medium of claim 15, wherein when the client browser receives said redirect message with the new URL, the browser dispatches a new request using the new URL to the server specified by the new URL.

17. The machine-readable medium of claim 15, wherein said redirect message is used to instruct the client browser to switch from Hypertext Transfer Protocol (HTTP) to Hypertext Transfer Protocol Secure (HTTPS).

18. A machine-readable medium that provides instructions, which when executed by a processor, cause said processor to perform operations comprising:

accessing a current URL used to locate HTML document currently loaded in one of multiple frames displayed by a Web browser;

building a new URL by concatenating https:// with the current URL; and

dispatching a new request using the new URL to invoke Hypertext Transfer Protocol Secure (HTTPS) communication between said one of multiple frames of the Web browser and a Web server.

19. The machine-readable medium of claim 18, wherein said instructions are embedded within a Hypertext Markup Language (HTML) document.

20. The machine-readable medium of claim 19, wherein the Web site is hosted by a plurality of servers coupled to a load balancer to receive requests dispatched by a Web page having multiple frames and distribute each request received to one of said servers.

21. The machine-readable medium of claim 19, wherein said HTTPS is automatically invoked when a client user enters a secured area of the Web site from an unsecured area.